CLAIMS

1.   A method for performing electronic trans-
5   actions, in which a sender of transaction messages is
assigned a smart card with an associated unique identity
and a private key stored in the card in a protected man-
ner, and in which an associated public key is kept gene-
rally available, c h a r a c t e r i s e d in that in
10   connection with an electronic transaction under the
sender's own control, preferably through his own input
of message information, the sender creates a transaction
message, which contains information necessary for the
transaction, and, in his smart card, provides the created
15   transaction message with his digital signature while
using his own private key for subsequent output and
transmission of the transaction message.

2.   A method as claimed in claim 1, c h a r a c -
t e r i s e d in that the transaction message contains
20   information on sender, receiver, amount and preferably
a transaction serial number.

3.   A method as claimed in claim 1 or 2, c h a r -
a c t e r i s e d in that the transaction message is
created off-line, i.e. not connected to the communica-
25   tions network that is used for the subsequent transmis-
sion of the transaction message.

4.   A method as claimed in claim 3, c h a r a c -
t e r i s e d in that the transaction message is created
off-line.

30   5.   A method as claimed in any one of the preceding
claims, c h a r a c t e r i s e d in that the transaction
message is created in the smart card.

6.   A method as claimed in claim 5, c h a r a c -
t e r i s e d in that the transaction message is created
35   with the aid of software inserted in the smart card in
advance and preferably also sender information inserted
in the card in advance.

17

    7.   A method as claimed in claim 5 ~~or 6~~, c h a r -
a c t e r i s e d in that information required for the
transaction message is input with the aid of input means
arranged on the smart card, the card preferably being a
5   so-called advanced smart card.

    8.   A method as claimed in ~~any one of~~ claims 1-6,
c h a r a c t e r i s e d in that information necessary
for the transaction message is input with the aid of a
protected card terminal.

10   9.   A method as claimed in ~~any one of~~ claims 1-6,
c h a r a c t e r i s e d in that information necessary
for the transaction message is input with the aid of a
separate card communication unit, the latter preferably
also being a card activator.

15   10.   A method as claimed in ~~any one of~~ claims 1-6,
c h a r a c t e r i s e d in that information necessary
for the transaction message is input with the aid of a
telecommunications unit controlled by the smart card,
especially a mobile telecommunications unit such as a
20   mobile phone.

    11. A method as claimed in ~~any one of the preceding~~
claims, c h a r a c t e r i s e d in that the transaction
message contains sender information in the form of at
least one of the following pieces of information: a card
25   number, a cash card number, a charge card number, a cre-
dit card number, an account number, an invoice number and
an ID number.

    12.   A method as claimed in ~~any one of the preceding~~
claims, c h a r a c t e r i s e d in that the transaction
30   message contains receiver information in the form of at
least one of the following pieces of information: a card
number, a cash card number, a charge card number, a cre-
dit card number, an account number, an invoice number and
an ID number.

35   13.   A method as claimed in ~~any one of the preceding~~
claims, c h a r a c t e r i s e d in that the signed
transaction message is sent to a card or account admini-

18

strator regarding the sender or receiver, that the digi-
tal signature of the transaction message is authenticated
by using the public key, which is assigned to the one who
is identified as sender by the transmitted transaction
5   message, and that in case of authenticity, the receiver
is credited with the transaction amount by a clearing
process.

    14. A method as claimed in claim 13, c h a r a c -
t e r i s e d in that the signed transaction message is
10   first sent to the receiver, who optionally after his own
checking of the digital signature of the message forwards
the signed transaction message to said card or account
administrator.

    15   A method as claimed in any one of claims 1-12,
15   c h a r a c t e r i s e d in that the signed transaction
message is encrypted by using a public key belonging to
the addressee, to whom the transaction message is sent,
that the encrypted, signed transaction message is sent
to the addressee, that the addressee by using his private
20   key decrypts the signed transaction message, that the
digital signature of the transaction message is authenti-
cated by using the public key which is assigned to the
one who is identified as sender by the transmitted trans-
action message, and that the receiver, in case of authen-
25   ticity, is credited with the transaction amount by a
clearing process.

    16. A method as claimed in claim 15, c h a r a c -
t e r i s e d in that the addressee is the receiver, that
the receiver, after decryption, sends the signed trans-
30   action message to a card or account administrator, where-
upon said authentication takes place.

    17. A method as claimed in any one of claims 1-12,
c h a r a c t e r i s e d in that the signed transaction
message is encrypted by using the sender's public key and
35   is provided with sender information and is then sent to a
card or account administrator, who has the sender's pri-
vate key and who preferably has issued the user's smart

19

card, that said administrator decrypts the received
encrypted message by using said private key, that authen-
tication of the digital signature of the decrypted trans-
action message takes place by using the public key, which
5 is assigned to the one who is identified as sender by the
transmitted transaction message, and that the receiver,
in case of authenticity, is credited with the transaction
amount by a clearing process.

18. A method as claimed in any one of claims 1-14,
10 c h a r a c t e r i s e d in that the signed transaction
message is sent non-encrypted, especially via a public
communications network, such as the Internet or a tele-
communications network.

19. A method as claimed in any one of the preced-
15 ing claims, c h a r a c t e r i s e d in that the signed
transaction message is sent by e-mail.

20. A method as claimed in any one of claims 1-18,
c h a r a c t e r i s e d in that the signed transaction
message is sent via a mobile telephone network, especial-
20 ly by using a so-called SMS service.

21. A smart card for carrying out electronic trans-
actions, comprising means for storing card identification
information, means for protected storing of a private
key, means for storing an asymmetrical algorithm, means
25 for input of transaction information into the card, pro-
cessor means for creating in the card a transaction mes-
sage based on input transaction information, such as
information on amount and receiver, and optionally infor-
mation stored in the card, such as information on sender
30 and preferably a serial number, and for providing the
transaction message with a digital signature on the basis
of said private key and said asymmetrical algorithm, and
means for output of the signed transaction message.

22. A card as claimed in claim 21, c h a r a c -
35 t e r i s e d in that it is of a so-called advanced type.

23. A combination of a smart card and a user-con-
trolled communication unit, which is arranged for commu-

nication with the smart card and with which the card is
adapted to be combined with a view to producing an elec-
tronic transaction message, the card comprising means for
protected storing of a private key, means for storing an
5   asymmetrical algorithm and processor means for providing
a created transaction message with a digital signature
based on said private key and said algorithm, and said
communication unit comprising means for input of trans-
action information, and means being arranged in the com-
10   munication unit and/or in the card for creating said
transaction message.

      24. A combination as claimed in claim 23,
c h a r a c t e r i s e d in that the communication unit
is a mobile telecommunication device.

15   25. A combination as claimed in claim 23,
c h a r a c t e r i s e d in that the communication unit
is a combined card activator and information inputter/
processor.

      26. Use of a smart card with a private key stored
20   therein for providing, independently of the communica-
tions network, an electronic transaction message provided
with a digital signature based on the private key.